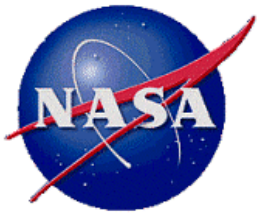


Software Quality Assurance (SQA) and Independent Verification and Validation (IV&V)

How They are Different and

Why Projects Need Both of Them for

Mission Success

Agenda

- Introduction
  - Scope
  - Frequently Asked Questions (FAQ's)
- Software Assurance 101
- NASA Software Directives
- Software Assurance Benefits
- SQA and IV&V
  - Complementary Disciplines
  - Fundamental Differences
  - Examples of Software Assurance Activities
- Office of Systems Safety and Mission Assurance (OSSMA) Challenges
- Summary

Introduction
Scope

- In response to Project questions and concerns, this presentation focuses on the roles and responsibilities of two Software Assurance disciplines, SQA and IV&V, their relationship to one another, how they are different, and why we need them
- Simple diagrams and examples have been chosen to highlight key differences and similarities between these complex disciplines
- While OSSMA currently lacks resources to implement a full Software Assurance Program, the Directorate is working to
  - Strengthen SQA and IV&V for GSFC programs (both ground and flight software)
  - Develop a Software Safety and Software Reliability program
  - Increase the level of Software Assurance expertise within OSSMA
  - Ensure GSFC Projects have the appropriate level of Software Assurance

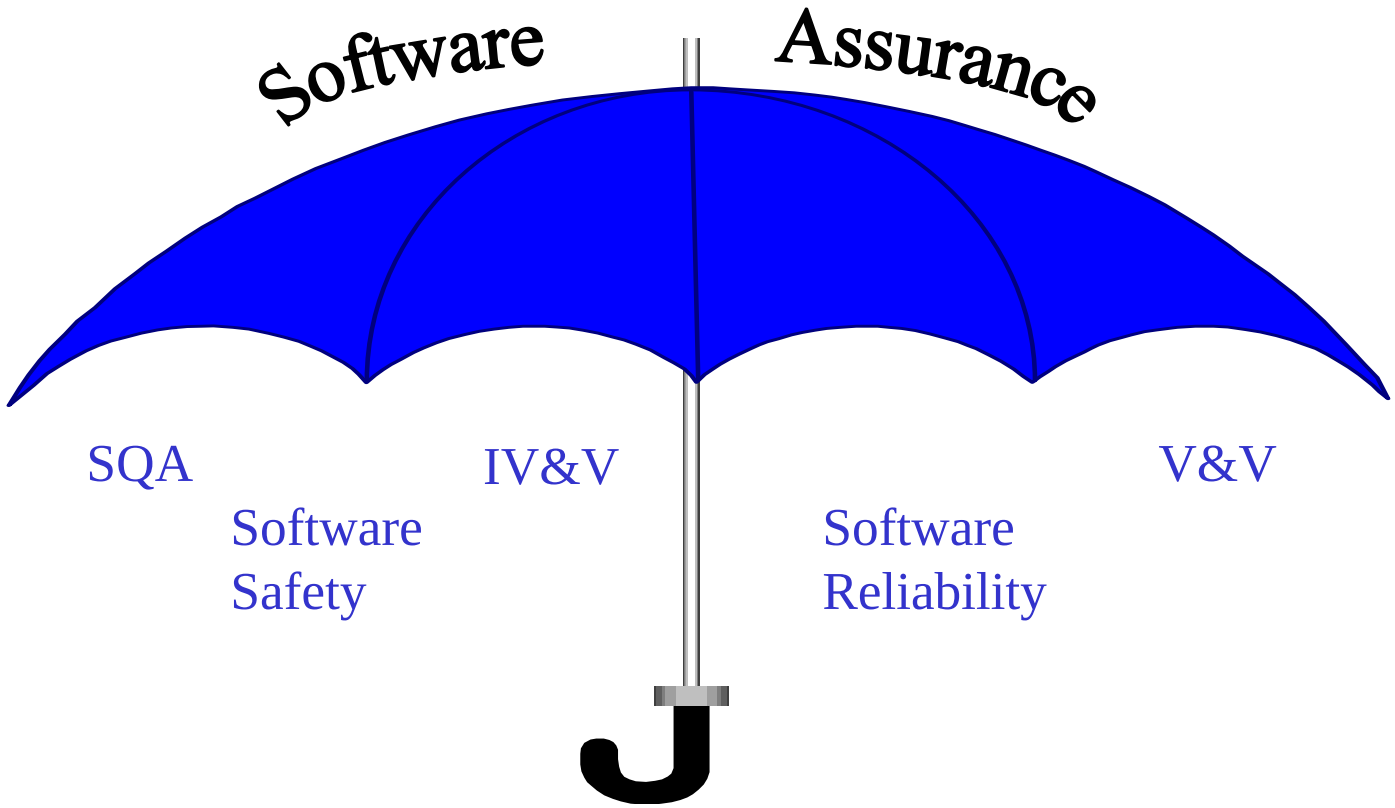
Introduction cont.
Frequently Asked Questions

FAQ's

- What is Software Assurance?
- Is Software Assurance the same as Software Quality Assurance?
- Are there directives that detail NASA's obligation towards Software Assurance?
- If I have IV&V on my Project, do I need SQA? Am I paying twice for the same thing?

Software Assurance 101

Software Assurance is an umbrella risk identification and mitigation strategy for mission and safety assurance of all NASA's software



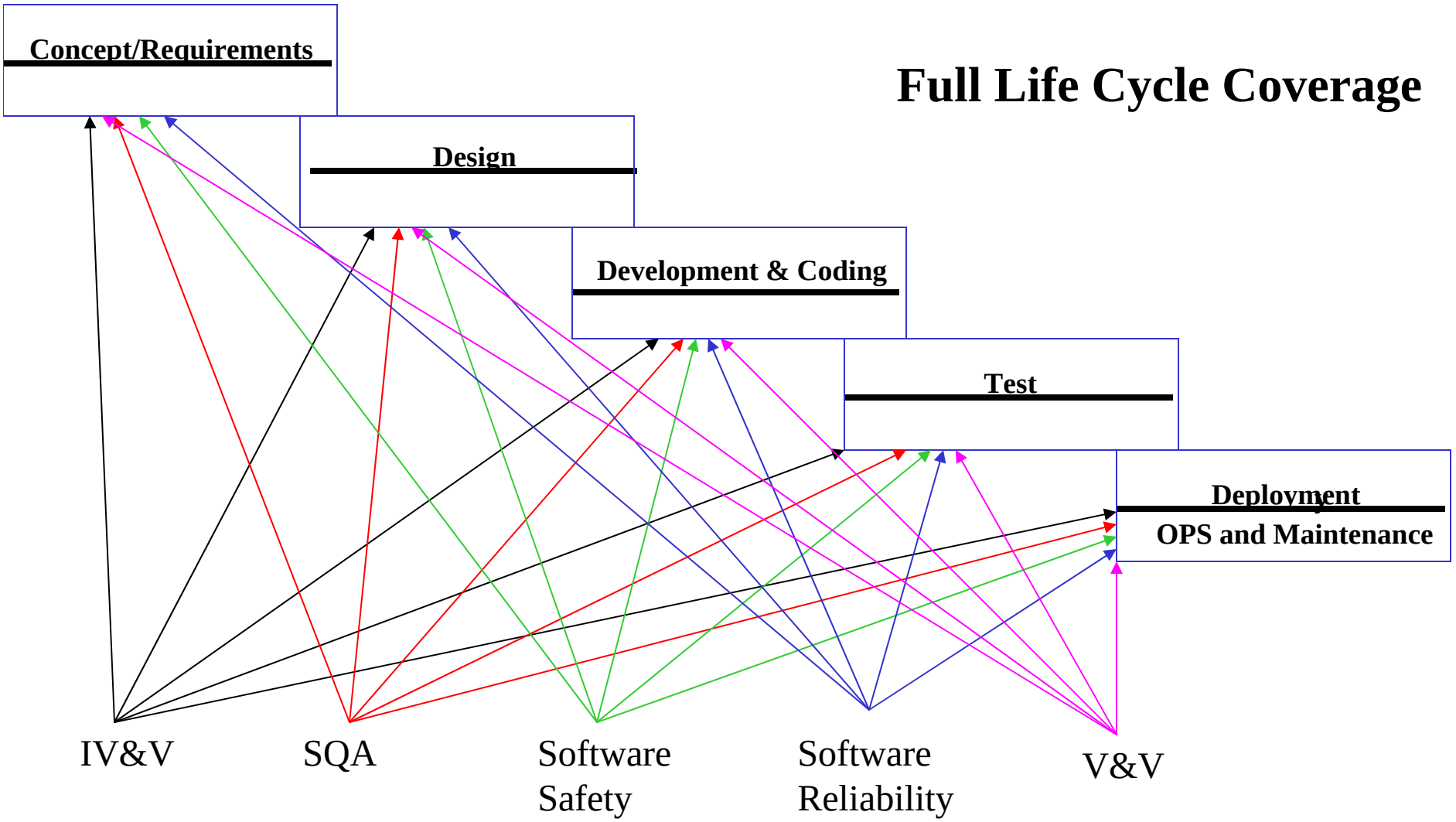
Software Assurance 101 cont.

- All Software Assurance disciplines strive to improve the quality of the product while employing risk mitigation techniques
- Each of the five disciplines performs distinct activities with unique evaluation perspectives
- The level of Software Assurance needed is dependent on the software size, complexity, criticality, and level of risk

Software Assurance is the planned and systematic set of activities that ensures that software life cycle processes and products conform to requirements, standards, and procedures. [IEEE 610.12]

Software Assurance 101 cont.

Full Life Cycle Coverage



NASA Software Directives
Related to Software Development

- NPD 2820.1 NASA Software Policies*
- NPD 7120.4 Program/Project Management
- NPG 7120.5 Program/Project Management Processes and Requirements
- NPD 8730.4 Software IV&V Policy
- NASA-STD-2201-93 NASA Software Assurance Standard*
- NASA-STD-8719.13A NASA Software Safety Standard*
- NASA-GB-A201 NASA Software Assurance Guidebook*
- NASA-GB-1740.13-96 NASA Guidebook for Safety Critical Software*

* Directives in blue are currently under revision

NASA Software Directives cont.

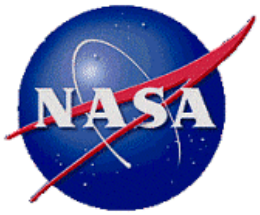
NASA Software Policy

Proposed updates to NPD 2820.1, NASA Software Policies, state that Centers shall:

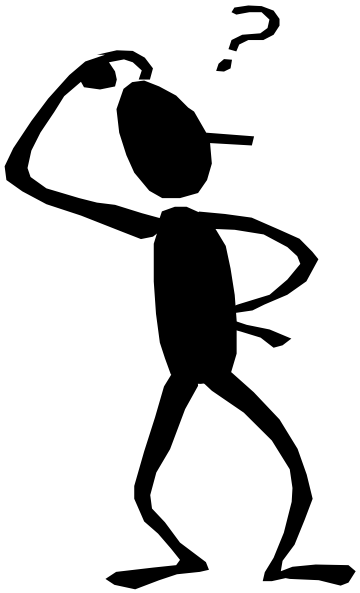
1. Implement a software assurance organization/program which operates independently of the NASA programs, projects and facilities it objectively evaluates.
2. Ensure that a Center Software Assurance Point of Contact is appointed.
3. Ensure that the appropriate Software Assurance representatives are members of the SWG, SEPG, and support those representatives.
4. Ensure that Center Software Assurance processes are developed, updated and reviewed.
5. Ensure that independent assessments of program and project Software Assurance processes are conducted on an as needed basis.
6. Identify the proper level of resources needed to perform Software Assurance activities for software development projects.
7. Ensure that Software Assurance personnel are properly trained.

Software Assurance Benefits

- Full life cycle Software Assurance activities provide independent and objective assessments of the processes and quality of the product (with time to react)
- Each discipline focuses on opportunities for early error detection, problem prevention, and risk identification and mitigation – earlier detection and identification yields fewer costs to fix and less schedule impact
- Software Assurance improves the quality of future products/services
- Information exchange between disciplines is necessary to maximize benefits!



"Aren't SQA and IV&V the Same?"



Complementary Disciplines

Definitions

- **Software Quality Assurance –** A systems process that evaluates processes and products with emphasis on monitoring processes to ensure the quality of the delivered product; ensures compliance to standards and procedures
- **IV&V –** A systems engineering process employing rigorous methodologies for evaluating the correctness and quality of the software product throughout the software life cycle

While SQA and IV&V may sound alike, they perform distinct tasks

- With complementary activities and results
- From differing levels of independence, objectivity, and reporting

Fundamental Differences

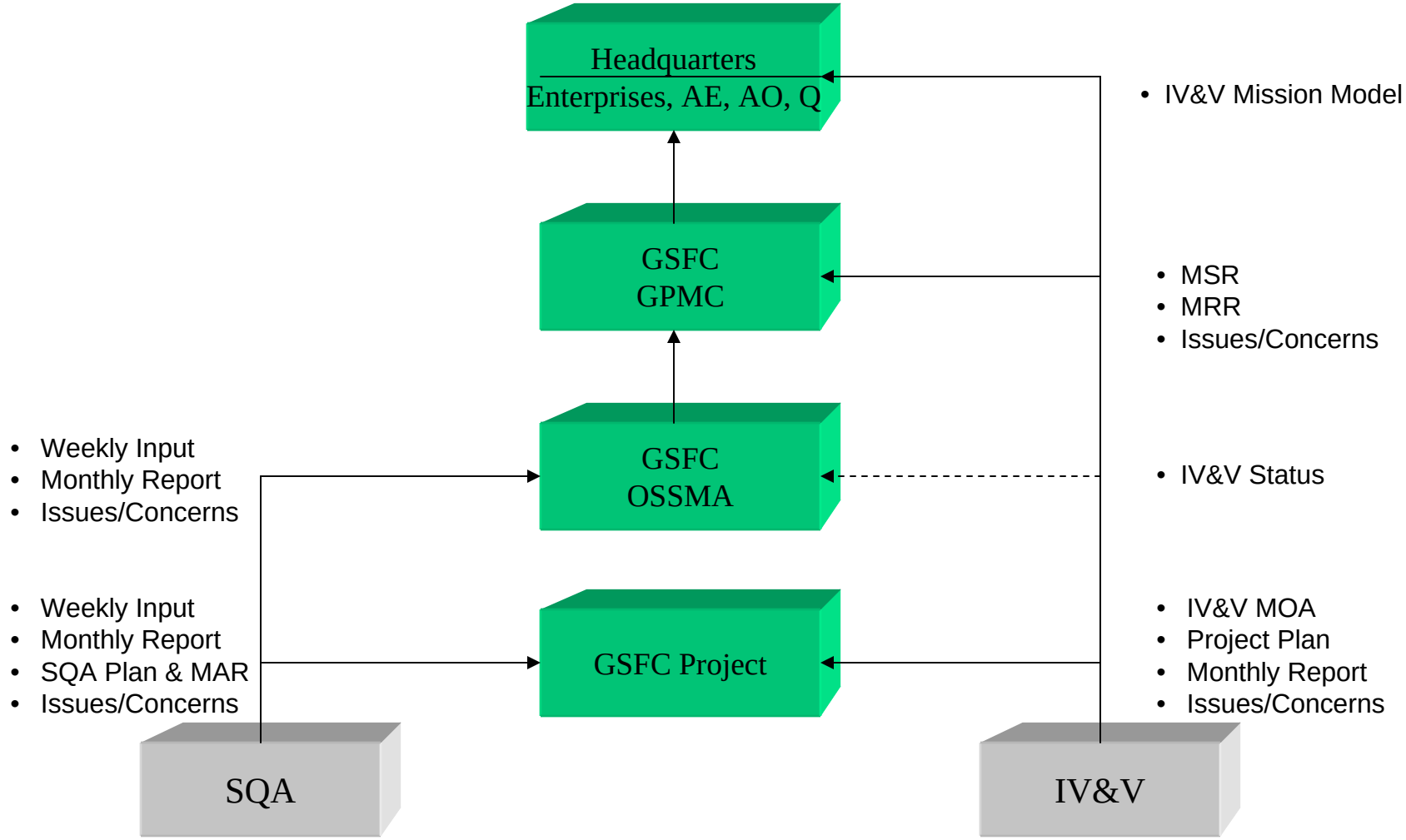
SQA

- Provides **Center-level** services
- Focuses on **ALL** Project software
- Emphasizes compliance to standards and procedures
- Reviews, monitors and audits all Project processes and products for completeness and accuracy
- Matrixed to the Project as part of the Project Team and provides daily insight/oversight
- Reports to Project and Center Director through OSSMA

IV&V

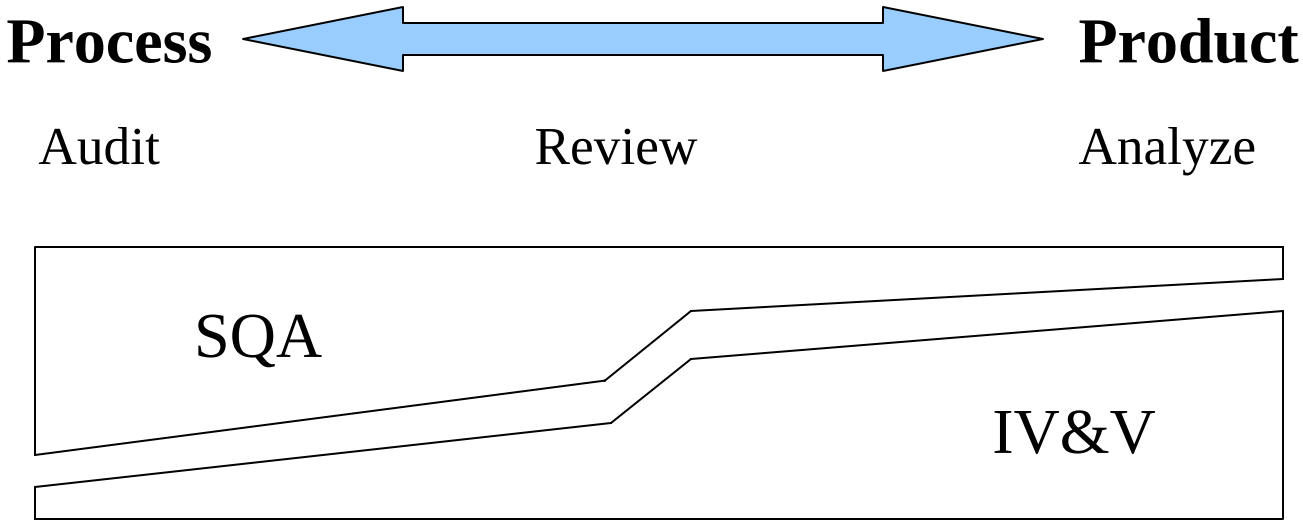
- Provides **Agency-level** services
- Focuses on **MISSION CRITICAL** Project software
- Emphasizes completeness and correctness of the product
- Reviews, analyzes, and provides in-depth evaluations of life cycle products which have the highest risk
- Independent from the Project and provides analyses and evaluations per IV&V priorities
- Reports to Project, GPMC's, and NASA Headquarters

Fundamental Differences cont.
Reporting Interfaces



Fundamental Differences cont.
Functional Characteristics

SQA and IV&V are complementary disciplines
(but neither supercedes the other)

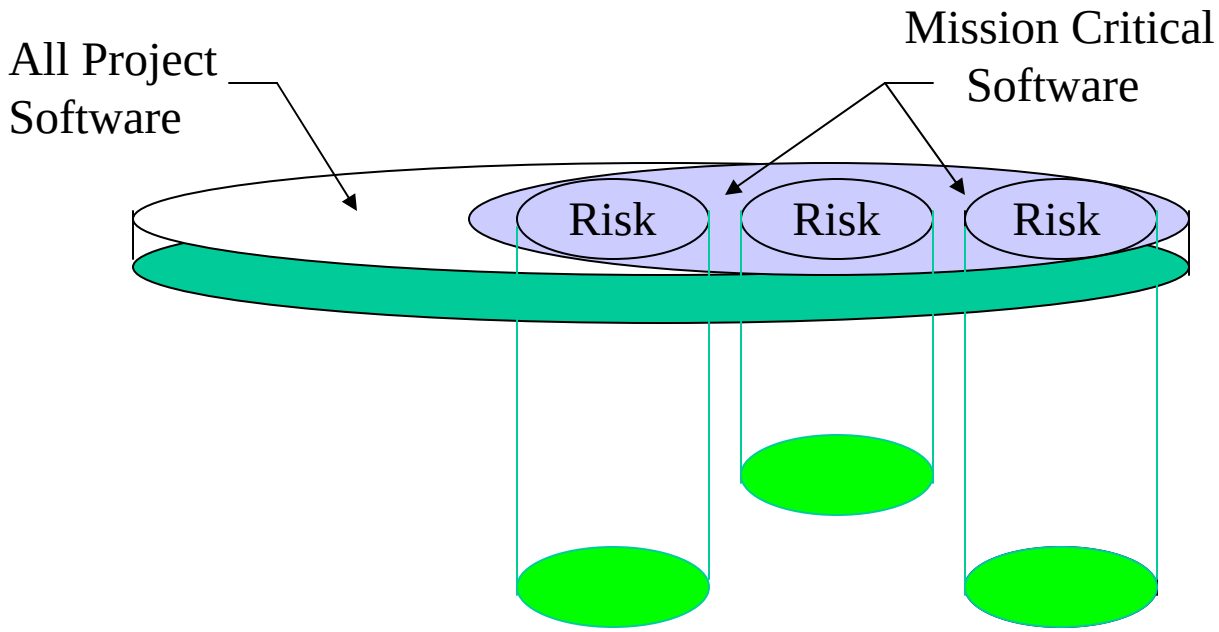


Compliance Consistency Testability Accuracy

Readability Completeness Correctness

(attributes from IEEE 1012)

Fundamental Differences cont.
SQA and IV&V Penetration



SQA (all software, review/audit)

IV&V (mission critical, risk based coverage/depth, review/analyze)

Level of analysis penetration by IV&V

Design Analysis

SQA

- Verifies design documentation meets intended purpose and has appropriate detail and all necessary elements
- Audits software development folders (SDF's) for completeness and accuracy
- Ensures configuration control of the design and requirements
- Attends design reviews/peer reviews from a **"process perspective"**
- Ensures design issues are resolved prior to next development stage

IV&V

- Validates ability of design to meet system needs/requirements
- Analyzes database design
- Performs design analysis of select critical algorithms
- Analyzes data flow, control flow, design testability and error handling
- Reviews developer prototypes or models
- Reviews or performs timing/sizing/loading analyses
- Attends design reviews/peer reviews from a **"product perspective"**

Examples cont.

Code Analysis

SQA

- Provides an analytical **snapshot of the entire software system** for programmatic decision making (at various points in the software development life cycle)
- Uses automated tools with minimal manual intervention for analyses and predictions
- Focuses primarily on the structural aspects of the software, identifying potential reliability risks based on complexity, size, branching, and internal documentation
- Assesses code complexity metrics for standards

IV&V

- Provides a **comprehensive analysis of selected code components** based on the complexity of the logic, use of new technology, or other criticality/risk factors
- Uses a variety of automated tools and manual techniques
- Verifies design compliance, data structures, logic structure and control flow, and error handling
- Assesses code complexity metrics for a risk assessment for prioritizing manual code analyses

OSSMA Upcoming Challenges

- Software Assurance standards and directives continue to change – Center Software Assurance Points of Contact are working with Headquarters to synergize efforts and to reach an Agency consensus on Software Assurance processes and best practices
- Project Management must be committed to Software Assurance
- OSSMA is strengthening it's Software Assurance approach to ensure consistency in its support to GSFC projects
- OSSMA is developing and infusing software safety and reliability as part of its system safety and reliability program

Summary

- Software Assurance disciplines are to be used to provide a consistent and comprehensive approach, process, and perspective for the identification and management of software risk
- The level of Software Assurance needed is dependent on the software size, complexity, criticality, and level of risk
- Each Software Assurance discipline employs different levels of independence, objectivity, and reporting
- SQA will be addressed on all GSFC projects developing or acquiring software
- IV&V will be assessed on all 7120.5 projects that include mission and safety critical software
- Correct application of and information exchange between Software Assurance disciplines is necessary to maximize benefits!

Summary cont.

- Early application of Software Assurance can positively impact cost, schedule, and technical decisions, while improving the quality of the products/services
- The Agency recognizes the importance of Software Assurance and is working to increase its visibility, strengthen NASA software policies, standards, and guidelines, and educate software practitioners and program management

✓ SQA will be addressed on all GSFC projects developing or acquiring software

✓ IV&V will be assessed on all 7120.5 projects that include mission and safety critical software

Epilogue

"So, are SQA and IV&V the Same?"